Designing for Trust in Blockchain Platforms

Zavolokina, Liudmila ; Zani, Noah ; Schwabe, Gerhard

Abstract: Trust is a crucial component for successful transactions regardless of whether they are executed in physical or virtual spaces. Blockchain technology is often discussed in the context of trust and referred to as a trust-free, trustless, or trustworthy technology. However, the question of how the trustworthiness of blockchain platforms should be demonstrated and proven to end users still remains open. While there may be some genuine trust in the blockchain technology itself, on an application level trust in an IT artifact needs to be established. In this article, we examine how trust-supporting design elements may be implemented to foster an end user's trust in a blockchain platform. We follow the design science paradigm and suggest a practically useful set of design elements that can help designers of blockchain platforms to build more trustworthy systems.

DOI: https://doi.org/10.1109/TEM.2020.3015359

Originally published at:
Zavolokina, Liudmila; Zani, Noah; Schwabe, Gerhard (2023). Designing for Trust in Blockchain Platforms. IEEE Transactions on Engineering Management, 70(3):849-863.
DOI: https://doi.org/10.1109/TEM.2020.3015359

This is the authors' version of the article. The printed journal version can be accessed at:
https://ieeexplore.ieee.org/document/9199099/

Designing for Trust in Blockchain Platforms

Liudmila Zavolokina, Noah Zani, Gerhard Schwabe

Keywords. Trust, Design Science Research, Blockchain.

Abstract. Trust is a crucial component for successful transactions regardless of whether they are executed in physical or virtual spaces. Blockchain technology is often discussed in the context of trust and referred to as a trust-free, trustless, or trustworthy technology. However, the question of how the trustworthiness of blockchain platforms should be demonstrated and proven to end users still remains open. While there may be some genuine trust in the blockchain technology itself, on an application level trust in an IT artifact needs to be established. In this study, we examine how trust-supporting design elements may be implemented to foster an end user's trust in a blockchain platform. We follow the design science paradigm and suggest a practically useful set of design elements that can help designers of blockchain platforms to build more trustworthy systems.

1. Introduction

Trust is a crucial component for successful transactions regardless of whether they are executed in physical or virtual spaces (e.g., online marketplaces) [1]. Blockchain technology is often discussed in the context of trust (which is claimed to be its main benefit [2]) and referred to as a trust-free, trustless (meaning that it eliminates need for trust between transacting parties), or trustworthy (meaning that it can be trusted because of its design) technology [3–6]. In recent years, it has attracted much attention from academics and practitioners. More and more blockchain implementations have emerged spanning different areas – from widely-spread cryptocurrencies [2] to rarer blockchain-based land registries [7] – to solve various real-world problems in which the presence of trust plays a crucial role.

Trust brought by blockchain technology is achieved by the transparent and immutable procedure of creating and storing transactions in a ledger [8]. However, the question of how the trustworthiness of blockchain platforms should be demonstrated and proven to end users still remains open [8]. While there are a growing number of research articles that address the technical design of blockchain systems (focusing on system architecture) or the fit of the technology in specific cases, there are only a few that focus on the user's perspective [9], which is essential when establishing the promised trust.

Certain factors hinder the end user's formation of trust in blockchain-based platforms, and therewith mitigate the benefits the technology may offer and hold back its acceptance and usage [10–13]. Amongst others, these factors include lack of experience with the technology and lack of understanding of how blockchain systems function, privacy concerns and liability issues [8, 10, 11]. In contrast to existing platforms where a user trusts one service provider, blockchain systems require trust in the whole community of users (in case of public blockchains) or in several service providers simultaneously (in case of consortium blockchains). Furthermore, there is no 'one-size-fits-all' blockchain technology: different design decisions [14] influence implementation of blockchain-based platforms and their final outcomes (e.g., usefulness for end users and ability to solve the addressed problems). This variety of possible 'configurations' calls for more careful investigation of design alternatives and their appropriateness. To leverage the benefits the technology offers and to foster its acceptance, these challenges must be overcome. While there may be some genuine trust in the blockchain technology itself, on an application level trust in an IT artifact needs to be established. To do this, trust-supporting design elements (TSDEs) can be implemented. These TSDEs represent single features or groups of features that positively influence the trust of an end user in an IT artifact [15]. In general, TSDEs are useful for trust building regardless of technologies because of their purpose of trust support. However, to achieve their promise, the appropriateness of particular TSDEs can be studied for particular technologies and types of applications. In this study, we take an exploratory approach and, using the example of a specific blockchain platform called "cardossier" (which we describe later in a corresponding section), examine which of trust-supporting design elements may be implemented to foster an end user's trust in a blockchain platform [13, 16]. Thus, we state the following research question: *RQ. What trust-supporting design elements foster trust of an end user in a blockchain platform?*

More specifically, we focus on the problem of the end user's lack of understanding of a blockchain platform (for example, about its purpose, functionality, etc.), which hinders the formation of trust [8, 10]. The study follows the design science paradigm and aims to suggest a practically useful set of design elements that can help designers of blockchain platforms to build more trustworthy systems. It is important to note that: 1) the research is initiated as a result of a problem which was observed in practice and in recent studies briefly covered by the literature; 2) the research is carried out as part of a larger blockchain design project, where researchers are involved in design activities, specification of requirements, and actual implementation of the system; and 3) the research does not aim to find completely new TSDEs, but to integrate pre-existing knowledge in the context of blockchain platforms and observe if such knowledge is useful to address the problem of the end users' lack of understanding.

The remainder of the paper is structured as follows: In the next section, we investigate the existing body of knowledge about trust in blockchain platforms with the focus on a user's perspective. Then, in the *Cardossier* section, we present the project and the blockchain platform that is our target for trust support. In the section *Research Method* we describe the process used in this research, followed by *Initial Requirements, Solution Objectives* and *Solution Components*. In the *Design and Implementation* section we describe the proposed TSDEs for the blockchain platform. This section is followed by *Evaluation*, where we present the results of feedback from end users, we collected. Finally, we discuss the results of this study and draw conclusions.

2. Related work

Trust in IT artifacts

Despite its importance, it is not easy to conceptualize trust, and there is no commonly accepted definition of it. One possible definition that reflects converging understanding is that trust refers to two components: 1) "positive expectations regarding the other party in a risky situation" [17], and 2) willingness to be vulnerable [18]. Other definitions mention the presence of uncertainty and risk, under which trust occurs. Trust plays an important role in different contexts: interpersonal relationships, organizational behaviors, conflict management, and business transactions [19–23]. By its nature, trust is inter-personal. However, the concept of trust has been expanded to IT artifacts and in recent years has been gaining importance in IS and HCI research. Scholars explore trust in IT artifacts (e.g., how it is established, how it changes over time, what factors influence it, what design implications we may derive to build up trust in systems, etc.) as it is of crucial importance for the acceptance and adoption of IS [24]. An IT artifact can play two roles in trust relationships: 1) the role of mediator between two humans, a trustor and a trustee, or 2) the role of a trustee, if the IT artifact is trusted in by the end user [25]. In this study, we explore the latter in order to come up with design ideas to establish the end user's initial trust in a blockchain platform by making it easier to understand. However, we acknowledge the importance of further research into how blockchain platforms change the way we trust other humans and institutions.

In the role of trustee, an IT artifact should directly build trust[1]. Antecedents of trust, explored in IS and HCI literature, can be used to inform trust-supporting design elements in information systems [25]. Understandability of how an information system works, transparency over how the output of a system was achieved, information accuracy, reliability of a system as well as explicit communication about system's activities are important antecedents of trust in an IT system [26, 27] to resolve issues associated with lack of knowledge, experience or understanding of a used system. These antecedents of trust lead us in our design of TSDEs in order to support trust formation in a blockchain platform.

Trust literature suggests that technology can transmit signals of trustworthiness as effectively as humans do [28]. Signals can help the trustor form expectations of trustee's behavior. They play an especially important role in first-time or one-time interactions, in which the trustor does not have any previous experience of the trustee or may have made inaccurate assumptions about them [28]. However, the presence of trust signals in the design of a system is not, in itself, enough to result in high levels of its perceived trustworthiness: their reliability and cost structure must be taken into account [28]. Good signals are considered to be easy and cheap to provide for trustworthy players and difficult and costly for untrustworthy ones [28]. Traditionally, trust signals in e-commerce and website design include reviews from previous customers, trust seals, references, and many more, widely known from the marketing literature. In our study, we use the concept of signaling trustworthiness to design the TSDEs for our blockchain platform.

[1] With this argument, we follow the cited HCI and IS literature. However, we acknowledge that trust in an IT artifact emerges from trust in the institutions and persons behind the artifact. Indeed, we see later that 'brands' are important trust-supporting elements. As this does not change the basic design insights of this paper, we stay with the more simplistic HCI and IS literature.

This is the authors' version of the article. The printed journal version can be accessed at:
https://ieeexplore.ieee.org/document/9199099/

Trust in blockchain technology

The discussion around the concept of trust in the context of blockchain technology has begun in design science research, HCI, and information systems in the past couple of years [6]. As the main benefit of the technology is claimed to be trust [2], there is a need to understand if and how trust relationships differ from existing concepts, and how this difference changes the design of systems. However, as the trust literature suggests [25], it is important to differentiate between trust mediated by technology (for example, transferring bitcoins from one individual to another without relying on a bank) and trust in the capabilities of the technology to fulfil its purpose (for example, trust of a bitcoin owner in the bitcoin network). The latter is a prerequisite for blockchain technology usage and adoption [2], and should be in place to enable trust between transacting parties mediated by technology [29]. Thus, in our study, we focus on how trust in blockchain technology may be established.

Earlier studies suggest that blockchain may a solution when establishing trust in cases where data integrity is an issue in records management, given that proper security architecture and infrastructure management should be in place [3, 8, 30]. However, the establishment of trust by blockchain technology is affected by certain limitations. For example, there is no guarantee that the stored data is reliable [30], and there should be additional mechanisms for data quality management [31]. In general, blockchain, as an infrastructure alone, does not suffice to instill trust in an end user: this should be established at an application level [32]. For this, certain design features, like an assessment of stored information or visibility of parties that provide this information, should be in place and adjusted to the certain business needs of an implemented platform [32].

Furthermore, trust in blockchain is hindered by a lack of technical understanding and experience [6, 10]. These factors, combined with the complexity of the technology and the potential for monetary losses due to them, cause feelings of insecurity and uncertainty among users, which then lead to difficulties in building up trust in the technology [10]. Some studies consider this factor to be the most significant barrier to the adoption of blockchain technology [33]. Though it is probably too early to properly research the adoption of the technology and its applications due to their immaturity and experimental character, we nevertheless acknowledge the existing need for additional trust support in blockchain platforms.

Examination of the existing trust in blockchain technology [34] suggests that it is not a new kind of trust that is being created (or changed fundamentally), but rather a shift from trust in one market player to others in the blockchain ecosystems. Thus, trust in the technology should be understood in known terms and established by traditional mechanisms [34]. Based on their study [34], we can conclude that institutional trust may play an important role in trust formation related to blockchain technology. Institutional trust can be defined as beliefs in the institutional mechanisms (e.g. contracts, regulations, legal recourse, or guarantees), which differ from trust in specific objects [35]. The information systems research suggests to differentiate between trust in technology and trust fostered by institutional mechanisms. Studies conclude that various institutional mechanisms (i.e., trust in seal programs) support technology and interpersonal trusts [1, 35]. In addition, a few studies explore the relationship between familiarity with an institution and trust in IT, concluding that the familiarity with an institution behind IT (be it an IT provider or an online vendor) increases trust in IT [36, 37]. However, the role of institutional trust remains unclear when it comes to blockchain platforms with their decentralized operation and governance. Does a trustless technology need to incorporate institutional mechanisms? What would be the institution to establish this kind of trust? These and many other questions related to the relationship between blockchain technology and institutional trust should be studied further.

Considering blockchain technology as an information system, we can differentiate between its three structures [38, 39]: deep structure (or also called a representation), surface structure, and physical structure. 'Deep structure' refers to a set of characteristics that describe a real-world system that an information system intends to model [40]. 'Surface structure' refers to the means of how a user accesses and interacts with an information system (for example, user interface, screens, menus, report layout). 'Physical structure' refers to the machinery that supports the two other structures (for example, a computer, a keyboard, a monitor, a network). The deep structure is accessed through the surface and the physical structures. Therefore, while the deep structure remains unchanged, the surface and the physical structures can be replaced or altered. In the example of an information system, which we refer to in this study, these three structures can be described as follows: (1) the deep structure is a trustful representation of a vehicle's history; (2) the surface structure includes interfaces through which a user accesses a vehicle's history; (3) the physical structure includes the device (a computer, a mobile phone) as well as the network which stores and transmits the necessary data about a vehicle's history. While the physical structure of a blockchain-based system brings inherent trust-building characteristics (such as immutability, reliability due to decentralized operation, transparency over transactions), the surface structure of a system can be used to communicate trustworthiness of such an information system. Burton-Jones and Grange suggest that learning the deep, surface and physical structures lead to more effective use of an information system [38]. Therefore, we aim to propose a set of design elements that, designed for the surface structure, can reveal the trustworthiness of the deep structure.

Enhancing trust in 'Black Box' technologies by explanation

In order to give the user a better understanding of the technology, an explanation should be given. It is not necessary to describe the technology in detail, but rather to explain the basic concepts and to help the user understand how the high-level functionality works. To achieve this, video tutorials or simple illustrations are often helpful. In website design, information components about a company and/or a product embedded in the site serve as external signals, helping to build trust [41]. These information components may also include information regarding how privacy and security measures are implemented as signals of the trustworthiness and benevolence of the service provider [41]. This type of information must be properly and promptly communicated. In our research, we explore what traditional signaling mechanisms, such as information components, may be implemented in a blockchain platform to enhance its trustworthiness.

An explanation is one of the methods in the design of systems for trust enhancement [42]. People tend to trust others when they explain why they do what they do [43]. Similarly, users understand a system better when the purpose and the process of a system are transparent to them. Especially, it is crucial in systems with higher levels of automation and decision-making, when the user can rely on the proposed decision only if he understands *why* this decision was proposed. Another example regards privacy. Given the recent introduction of privacy regulations (i.e. the GDPR, introduced in the EU in 2018), a meaningful explanation that helps a user understand how her personal data is being handled by businesses (e.g. for creating personalized offering or advertisement) might become a legal basic human right, i.e. 'right to explanation' [44], going hand in hand with the 'right to be forgotten'.

The transparency about the purpose and the process of a system improves an end user's understandability about the system, and, thus, addresses one of the important trust antecedents, discussed above [26, 27], i.e. understandability. It might seem that the more explanation about a system's functioning (i.e. its purpose and process) is given and, the more transparency is provided. The more transparency might mean the better understandability of a system, and, consequently, the more trust the user experiences. However, various factors break this relationship. For complex systems (e.g. expert systems, security-sensitive systems, AI systems, or autonomous-driving systems), additional information, on how a system works, may not influence a user's trust perception, but even impede trust. For example, Kizilcec [45] studied how a transparent design of algorithmic interfaces can promote awareness and foster trust. In his experimental study, he discusses the critical role of user expectations about system output and provides empirical evidence for a bell-shaped relation between transparency and trust. Additional information (i.e. more transparency) was confusing and reduced understanding of a user instead of opening the 'black box' [42, 45].

The concept of 'black boxes' is mostly discussed in relation to complex systems. Pieters [42] define 'black box' as 'something that outputs something based on certain inputs, but that we do not know the inner workings of'. From a user perspective, 'black box' systems are characterized by a lack of visibility or observability and missing explanations. Pieters [42] discuss an explanation of AI systems and its influence on trust formation. He concludes that to foster trust, given explanations should be not too little (if only *why* is addressed, but *how* is hidden, and thus, failing to open a black box), and not too much (which would make a system incomprehensible and a user unable to process information which is too detailed for her cognitive abilities or prior knowledge). Thus, a balance in the level of provided information should be found. While blockchain technology, that is in the focus of this study, is certainly a complex technology that is not well understood by an end user, the question remains open whether or not it should be black-boxed or, in contrast, white-boxed to foster the trust of an end user, and how this may be done.

Blockchain technology in the used-car market

The used-car market is known as one suffering from a lack of trust from its consumers. The everyday situation of experiencing much of quality uncertainty and information asymmetries while buying a used car is very much familiar to an average adult person. This situation, leading to complete extinction of good cars on the market, was described in 1970 as a 'Market for Lemons' problem by the Noble Prize winner G.A. Akerlof [46]. To address the 'Market for Lemons' problem, such measures as guarantees, regulations, certifications, history reports are introduced. A vehicle history report is the focus of this study. Today, history reports, like ones offered by Carfax, are collected from public sources and struggle with the lack of data quality (due to its incompleteness and incorrectness) and thus cannot be fully trustworthy. In recent years, more and more studies referred to blockchain technology as one of the possible solutions to address information asymmetries, quality uncertainty and missing trust in the used-car market. Notheisen, Cholewa, et al. [47] addressed the problems of information asymmetries in the car market by implementing a proof-of-concept prototype to gather the history of a real-world asset (a car) in a blockchain-based system and showed the feasibility of this solution. As such, this blockchain-based solution offers a more secure and reliable, and thus trusted vehicle history report due to the technology's capabilities of authenticating data [7] and distributed data collection. In contrast to traditional (Carfax-similar) solutions, a blockchain-based solution differs in the way it collects and stores data. In blockchain-based solutions, car data is collected by various organizations from a car's life cycle as well as dongles or sensors installed in a car without a need for any central authority. It is then timestamped and recorded in a blockchain system, which makes this data immutable, data providers transparent, and the overall control over the system distributed between its participants. Altogether, this process makes data more trusted. Simulating the used-car market, Bauer et al. [48] demonstrated a positive impact of the trusted car data both for buyers and sellers. Similar projects emerge in different domains, led by both academia and practice. For example, there are blockchain solutions for land registries, provenance, supply chains [11], which reduce information asymmetries and mitigate fraud by introducing authenticated, transparent, and more trusted data. However, most of them target businesses as their primary customer. While for some of them (for example, in supply chains) private users are not relevant, and businesses possess enough understanding about blockchain technology, for others involving private users in the design and assessing their needs may be a crucial factor for future adoption.

3. Cardossier

This study is part of a larger action design research project [49], called the Cardossier project. The project runs in Switzerland and is designed by a consortium of companies from the car-related ecosystem: an insurance company, a car dealer and importer, a car-sharing company, a road traffic authority, a software company, and two universities. In March 2019 a non-profit association was founded to foster market expansion and further development of the platform. New players from the car-related ecosystem joined the association. Together, these companies are implementing a so-called cardossier platform that encompasses a car's history over its entire life cycle, from the moment of production to the moment of disposal. The primary goal of the cardossier project is to reduce information asymmetries in the used-car market, to digitalize and improve the processes, minimize redundancies, and establish a trusted ecosystem for car-related data management between all the players involved into the life cycle of a car [31, 32, 47, 50]. Figure 1 shows the architecture of the cardossier platform. Cardossier Core is a blockchain-based storage for data exchange (in our case, based on Corda, a permissioned distributed ledger). The cardossier Dapp store provides a framework for so-called Dapps (decentralized applications). These Dapps access and utilize the authenticated car-related data and can execute business logic (for example, to create an insurance police, for fleet management, or other use cases). The Dapps are then connected to external systems, such as web portals (for example, an online portal for used cars), web applications, or other systems. In this study, we focus (marked as purple in Figure 1) on the design of TSDEs for the interface application that includes the dossier of a car to support the end users. We further refer to this prototype for the interface application as cardossier app. Another application that was developed in the course of this study is cardossier game (marked as blue in Figure 1), we explain it in the next section. The cardossier platform architecture does not reflect the physical structure (the blockchain network, computers), but demonstrated the surface structure – at the top level as interfaces to the car-related data provided, and the deep structure which spans between the cardossier core and the Dapp stores with its use cases.

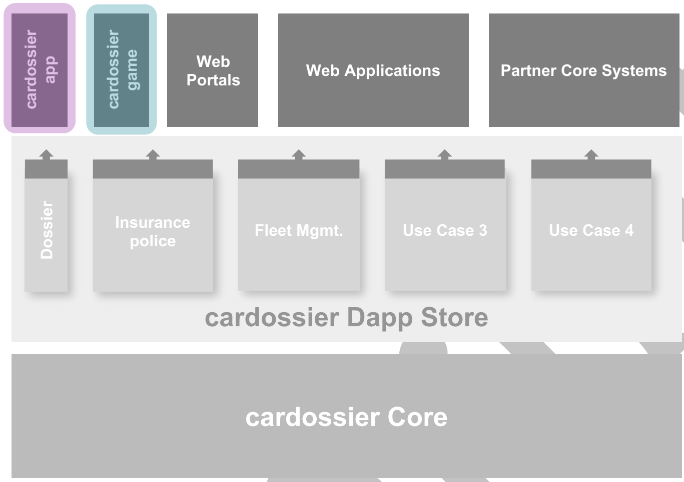


Figure 1. Architecture of the cardossier platform

Though the project has several facets which are crucial considerations for the design of the platform (like platform governance [51, 52], business model [50], incentive system [31], blockchain consortium management [53]), we focus on its application level and the perspective of its end users: car buyers, willing to consult the cardossier to assess the quality of a used car they intend to buy. Prior studies report on the problems and needs of car buyers [32], where additional trust support in an application design and sense-making of blockchain-based data are favorable [54]. This simple scenario gives an idea of a setting in which the cardossier platform is used by a car buyer: *Max, a 45-year-old plumber from Zurich, intends to buy a used car. He searches on an online portal UsedCarsPortal.ch for a 5-year-old VW Golf, which is offered by Nancy. Max contacts Nancy to check whether the information about the condition of the car corresponds to what is published online. Nancy mentions that there is a* *blockchain-based cardossier available for the car, which may convince Max that the information she has provided is genuine. Max is interested in viewing the cardossier, however, he is not sure whether he can trust it either: he has not heard about blockchain before.* To leverage the value of the capabilities and benefits the technology may bring to Max, there should be additional clarification of what makes the platform trustworthy and why Max can rely on it. This serves as a starting point for the design of the current study. The upcoming chapter explains how the TSDEs were designed to support the end users' understanding of the cardossier, establishing trust and helping Nancy and Max to complete the deal confidently and efficiently.

4. Research Method

The development of TSDEs follows the design science paradigm [55–58]. Design science research is aimed at finding new solutions for both known and unknown problems [59, 60]. Solutions produced by design science research should be applicable to resolve classes of problems and thus be generalizable [49]. While the design science cannot, on its own, provide sufficient evidence to support developed hypotheses, its activities often help to formulate the hypotheses and initially filter out those which are not worthy of further development [61]. No specific order is imposed when moving between the world of specific problems and solutions, and the world of general problems and solutions [61, 62]. Design science researchers may start with the creation of a specific solution for a specific problem and then generalize it, or work the other way round by starting from a generic problem, creating a generic solution and then applying it to a specific problem to demonstrate its value [49, 61, 62]. In this study, we took an exploratory approach, used a mixed strategy and combined techniques from design thinking [63] and design science research. This research originates from a specific problem that we observed in the cardossier, is abstracted to the problem of users' resistance to use the platform due to lack of understanding of blockchain platforms. We admit that this problem is not unique for blockchain applications and not the only one which may hinder adoption but one of possible problems. However, it is very prominent given the complexity of the technology. As is typical for DSR projects, the development takes place in multiple design-evaluate iterations [64]. This overall illustration of the generic and specific domains for the problem and the solution in our study can be found in Figure 2. The generic and specific solutions and the process, how they were defined, are described in more detail in the next sections. The steps, described further in this section, are summarized in Figure 3.

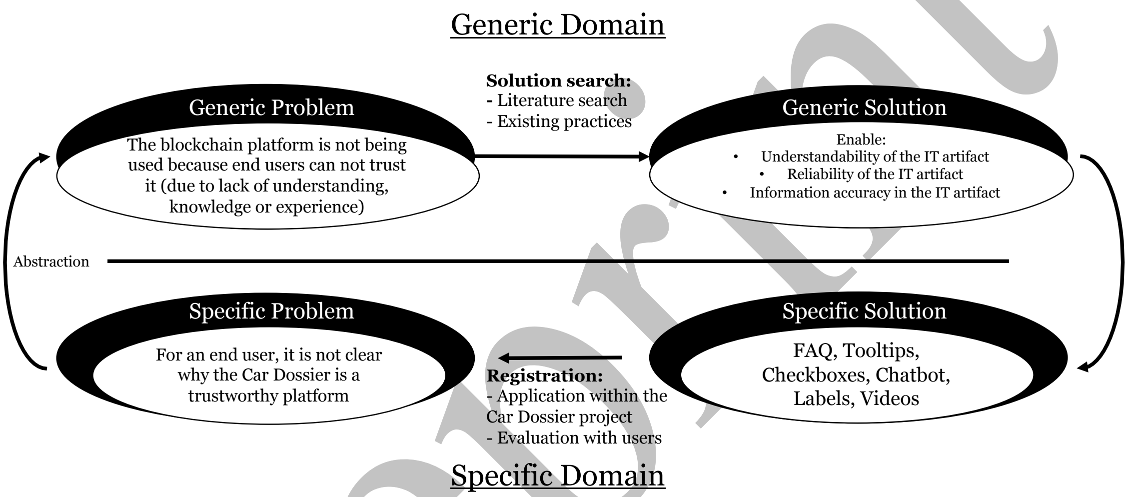


Figure 2. Generic and specific domains in the design

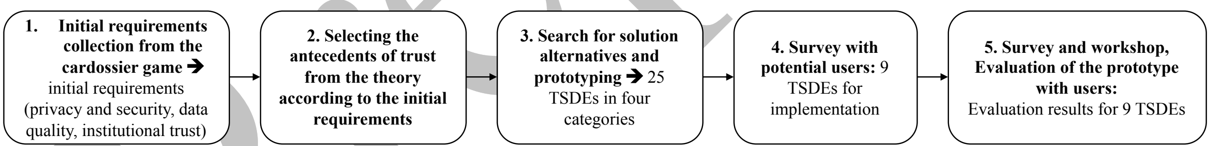


Figure 3. Steps undertaken in this study

Initial requirements collection – cardossier game

As a first step, to get a better and more detailed understanding of users' needs and select relevant antecedents of trust to be addressed, a used car market simulation game (cardossier game[2]) was developed (marked as blue in Figure 1). In the game, an early cardossier prototype was integrated into an online platform. The cardossier game helps designers of the cardossier early-on inform their design decisions by providing a very realistic environment, i.e.

[2] We do not provide a very detailed description of the cardossier game as it is not central for the current study. However, we encourage the reader to consult the manuscript [48] which describes in detail the design of the cardossier game.

interaction of users on a platform that is familiar to them. The participants in the game were randomly assigned to one of two groups: car sellers and car buyers. Each group had an equal number of players. Both groups received a scenario and a budget for the game. For both buyers and sellers, the goal in the game was to maximize the relative revenue. During the game, participants could get access to the cardossier for any available car to be able to better estimate the actual value of the car. The cardossier included information from two categories: (1) data (vehicle data, repairs and services, and driving dynamics), and (2) analysis of this data (which revealed the influence of specific data elements on the value of a car in comparison to the market price). Figure 4 shows a screenshot of the user interface used in the game.

The game took place in June 2018 at one European university. 48 BSc information systems students participated in the game. 80% of the participants were male. 27% of the participants had already experienced buying a car via an online used car marketplace. Directly after the game, the participants were asked to provide their feedback about their experience in the game and perception of trust in a semi-structured interview [48]. The interviews were recorded, transcribed, and coded.

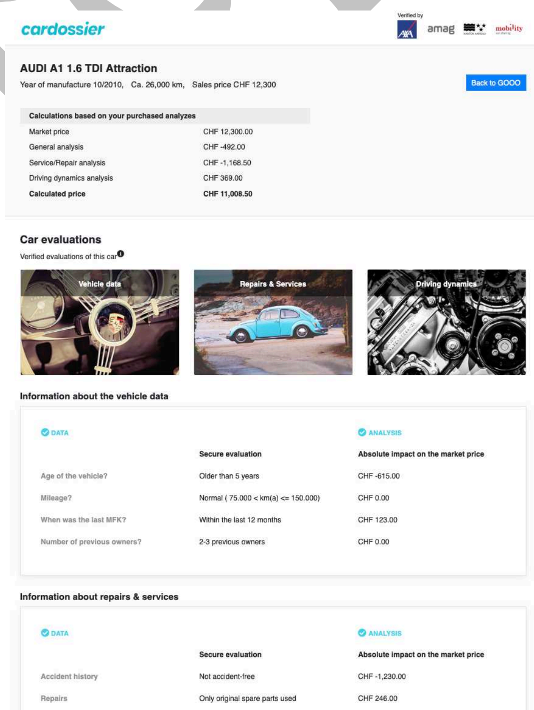


Figure 4. A cardossier with data and analysis information

The coding of interviews is a common approach for data analysis in qualitative research [65]. "A code in qualitative inquiry is most often a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data. [65]" The coding process was done by two researchers, using open coding in the MAXQDA software. To minimize the chances of errors from coding, ensure inter-coder reliability and internal validity, the researchers cross-checked the coded segments several times during the coding process. 71 data-driven codes (codes that emerged from the documents themselves, and not the ones predefined by a theoretical framework) were derived from this process. These codes were used to assign sentences and groups of sentences with a specific meaning (reflected by a code). We call these sentences and groups of sentences 'coded segments'. The codes were subsequently merged under specific themes by making connections between the data and the theory on trust. In total, 573 segments were coded. Table 3 in Appendix provides an example of coded segments for the sub-codes 'falsification'. Table 4 lists the codes used for the analysis of the interviews as well as the number and percentage of the coded segments[3].

Search for solution alternatives and prototyping

The next step involved a broad search for pre-existing solutions to problems of a lack of understandability and trustworthiness in a website and system design, which included literature research and exploration of existing practices. An extensive list of possible ideas for TSDEs was generated. No specific criteria or restrictions regarding the feasibility of the components were set. The result was a list of 25 TSDEs, which was then further refined in subsequent

[3] Due to space limitations, Table 4 is available under the link: https://drive.google.com/file/d/1tAaW1YdZx-cwHn_fe4UalEttfI23Gwch/view?usp=sharing

steps. To reduce the wide variety of TSDEs to a smaller set of feasible TSDEs, a short survey[4] was created. In total, 22 respondents aged between 20 and 49 (12 female, 10 male) participated in the survey. The survey intended to identify TSDEs perceived as important and relevant, and to exclude those that were perceived as inappropriate or unhelpful. To make the survey more comprehensive, we grouped the 25 TSDEs into four categories. The selected categories were *user interface, soft factors, labels,* and *information*. The participants were asked to rank the TSDEs in the preferred order of importance or relevance. Based on the feedback from participants of the survey, for a more realistic setting, it was decided that the TSDEs should be consistently embedded in the cardossier integrated into an online used-car sales website. This provided familiarity with the situation (by eliminating possible distractions caused by completely new software) for future evaluation participants. As a next step, the identified TSDEs that were seen as valuable were mapped to the antecedents of trust, that were selected to be addressed after a literature review and collection of initial requirements in the cardossier game (we discuss this selection below).

Evaluation

Evaluation is an important step in DSRM. Through evaluation, a design researcher tests whether or not the design goals of the IT artifact were achieved [56]. In our study, we focused on qualitative results to get deeper and richer insights in trust formation and related concepts. These insights do not imply any correlation or causation between the concepts, but might serve as a useful basis for further theory development.

First iteration – Survey and Workshop. The nine prototypes of the TSDEs were created with a wireframe tool: Balsamiq. The created prototypes were then evaluated in another short survey. The aim of the second survey (completed by the same participants) was to further test the components found to be most important or relevant in the first step by enhancing them

[4] The surveys referred to in this paper can be provided upon request.

with visual information, enabling the participants to see the prototyped TSDEs. These were then refined in terms of their feasibility and design in a workshop with the cardossier project team (the workshop took place in July 2018, with 16 project members). After this process, the final most relevant TSDEs were chosen to be implemented in the cardossier app, a web-based application.

Second iteration – Evaluation with Users. The implementation of the TSDEs was evaluated by nine participants aged between 20 and 50 (5 female, 4 male). During the evaluation of the TSDEs' implementation, each participant was provided with a scenario that they were asked to role-play. Each person was a customer who wanted to buy a used car because they had changed their job and needed to commute to work. They had already selected a car on an online platform. They saw that a cardossier existed for the car and that some of the displayed data originated from it. Now that they were aware of it, they wanted to find out more. In order to establish whether the TSDEs helped to improve understandability and perceived trustworthiness of the system, each participant was asked to use the platform and answer two of several questions (about the team, functionalities of the cardossier, its business model, and how their personal data was handled). The order of TSDEs to be tested and the choice of questions to be answered per TSDE were different for each participant to diminish the learning effects. To capture a deeper understanding of the feelings the users were experiencing, semi-structured interviews were conducted immediately after the test. These interviews were recorded, transcribed, and coded, using MAXQDA software for qualitative research. The coding process was done by one junior researcher, using open coding, and then iteratively discussed with and checked by a more senior researcher in a series of regular meetings for three months. This helped to resolve any uncertainties regarding codes or coded statements during the coding process.

This is the authors' version of the article. The printed journal version can be accessed at:
https://ieeexplore.ieee.org/document/9199099/

5. Initial Requirements, Solution Objectives and Solution Components

Initial Requirements

In this section initial requirements, mentioned by the participants of the cardossier game in the interviews, are presented. These requirements were mainly focused on *what* information should be communicated to the end user so that the user perceives more trust in the IT artifact. Participants of the used car market game highlighted several important topics that should be at least to some extent addressed and communicated in the interface: privacy and security, data quality, and institutional trust.

Privacy and security. Privacy and security were important to the participants. However, no detailed explanation is required about how exactly the data is encrypted by the technology, but users await a general indication that the system is secure. In terms of privacy, however, more detailed information is expected to be provided. For example, one participant said: 'You may say that the technology behind is secure and no one can hack the system, or so. I mean, I hope it is, it is just the owner of the system who confirms it. In terms of privacy, I would definitely show which data will be stored and for how long. Now for example, if I do a post on Facebook, or if I, don't know, if I don't delete it, then it's there forever. So that one simply has this clarity and understanding, what happens to my data if I delete my account. What data exactly is deleted? What data does remain?' (I25)[5]. Some of the participants expressed skepticism regarding privacy handling and highlighted the need for incentives for data provision, one participant said: 'I'm rather skeptical about such promises regarding privacy and whether or not they're really followed. If they [the project partners in the cardossier] would really just analyze my driving data and see that I am driving decently so that there is a premium reduction, then I would use it [the cardossier]' (I4).

[5] The quotes here and further in the text are taken from the interviews, where I1 – I48 indicates the participant number.

Data quality. Besides privacy and security, most of the concerns were related to the quality of car-related data, provided in the cardossier. Therefore, the participants highlighted the need for answering the following questions about this data: who the provider of this data is, how this data was collected, who has control and can manipulate this data, what the incentives of data providers are, whether the data is complete, whether any party can verify the data and confirm its quality. For example, one participant commented: 'I think I'd like to get information in advance on how the whole dossier is being created. I know that this is the dossier in which I now have the data, and I would like to know how the data is collected. Whether this is now somehow a recorder that is installed in a new car and records the whole thing or something. I think that knowing exactly what it is, how exactly the data is recorded, influences my decision as to how much I would trust that data' (I16).

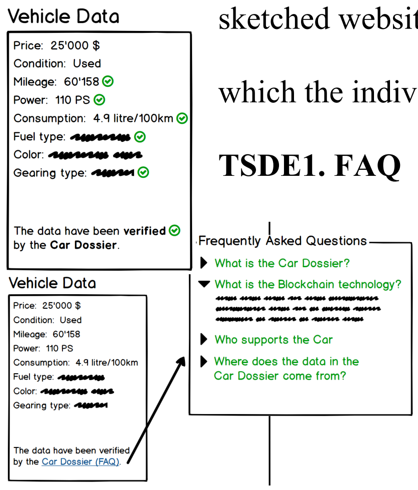
Institutional trust. Finally, the participants stated that the visibility of organizations that support the cardossier, or confirm the validity of certain data would enhance their trust in the application. For example, one of the participants said: 'If you show that some larger companies could confirm the data, it would be much more trustworthy. It's not like only one person records whatever he wants and shows it as a proof' (I45). Another participant claims: 'I think if it [the cardossier] is provided by a trusted entity, then I would trust it absolutely' (I28). He then continues: 'Also the label of the university and the cooperation with a governmental authority – this is already some kind of guarantee, which would positively influence my level of trust.' (I28) Several participants highlighted the importance of support from the government. For example, a participant provides the following argument: 'I would probably trust the cardossier much more if there is a state institution behind it, than if it is a private business. Simply because this state institution doesn't really aim to maximize its profit or so. And because the state also depends on people ultimately trusting the state. So, I would probably trust the state more than an importer, a profit-maximizing company' (I16). However, there were also opinions that question trustworthiness of shown logos or labels in the interface: ‘If there's just the logo on it now, I'd be ready to say it is trustworthy. However, if you think about it, it doesn't say anything at all. If it's a real car purchase which costs me a lot of money, I'd probably look at the official site of this institution that provides its logo or a label, whether it's really a real thing that they publish there’ (I11).

Solution objectives and solution components

As mentioned before, we started from a specific problem observed in the blockchain project. We found confirmation of this problem in the recent IS literature [10, 33]. The generic solution is informed by three antecedents of trust [25]: understandability, reliability, and information accuracy that were chosen after the consideration of the analysis of the user needs and initial requirements, described above. More specifically, the antecedent *understandability* was chosen to address the general need of users to get information about the IT artifact’s functioning (summarizing all three topics in requirements). The need for privacy and security as well as the requirement about the institutional trust determined the choice for *reliability* antecedent. Finally, the requirements for data quality in combination with the institutional trust determined the last antecedent, *information accuracy*. These antecedents lead us in the design of our specific solution, where we illustrate specific TSDEs, developed for the cardossier.

6. Design and Implementation of TSDEs in the cardossier app

The TSDEs selected after the first survey are described further in the order they were presented in the survey. These TSDEs were designed for the cardossier app (see the cardossier app on the platform architecture in Figure 1). TSDEs in the user interface category (such as "Embedding the information in a known system", "As much information as possible at a glance" or "Keeping the design as lean possible") were not implemented as separate TSDEs but were followed as guidelines for the prototyping. As a starting point in the design, a

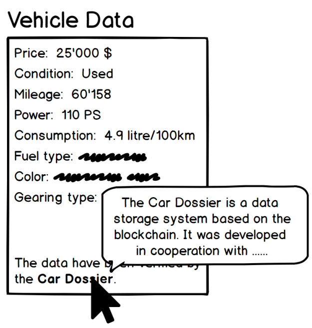


sketched website for an online used-car sales platform was created, into which the individual TSDEs were embedded.

TSDE1. FAQ

FAQ is a mechanism mainly used in e-commerce to provide information about a service or a product in a way that is easy to understand (by answering frequently asked questions), thus helping to resolve issues in understanding [66]. FAQ can be accessed via an embedded link. It encompasses frequently asked and relevant questions regarding the cardossier and answers to them. It includes the following categories of questions: general (e.g., what the cardossier is, who its users are); financial (e.g., how the cardossier is financed, how much the cardossier costs); data and privacy (e.g., what data is collected, how it is processed, how data privacy is achieved); and technical (e.g., what the technology behind the cardossier is, what functionalities the cardossier offers).

TSDE2. Tooltips

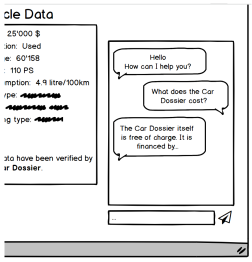


Tooltips is a way to extend user knowledge with additional information in case they need it [67]. The tooltips make it possible to show predefined content when the user moves their cursor over a certain element of the website. In the example shown, a short explanation is displayed when the user navigates their cursor to the words “Cardossier”.

TSDE3. Checkboxes

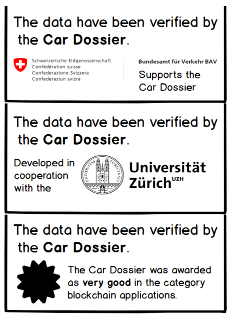
Checkboxes (also called checkmarks) are a simple way to reflect a positive or a negative quality, which goes along with ratings in e-commerce [28]. They help the end user to better understand if a product (in our case data) is of good or bad quality. The checkboxes make it possible to show which data came directly from the cardossier when the end user views the information through a third-party sales platform and not on the cardossier platform itself. When viewed on a third-party platform, the end user sees checkboxes next to the 'verified' data together with a note or legend. If the end user were to view the data directly on the car-dossier platform, the checkboxes would be obsolete because all data would have a check mark.

TSDE4. Chatbot



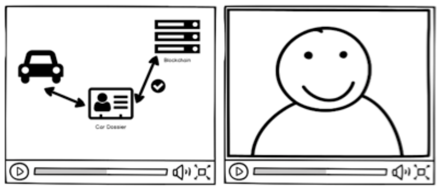
A chatbot can help by answering questions a user might have in real time. Though it provides the very same information as the FAQ does (in our design), it simulates a conversation with a person which is appealing for a user in terms of trust under the condition that the chatbot reacts as naturally as a human does [68]. A question can be written and submitted in the text field. Based on this, the chatbot can then check the question against a database with predefined content and provide a corresponding answer. In the example, the chatbot uses the same questions that are used in TSDE1 FAQ.

TSDE5 – TSDE7. Labels (governmental / university / certification)



Labels are powerful trust signals [69] because they can show that an organization supports the development of the application, or ensure validity of the provided data. Thus, trust in this particular organization (if it is a reputable and trustworthy one) is transferred into the application. The first possibility is a governmental label such as the label of a federal office, that supports the project. As part of this possibility, another conceivable option would be the label of one or several regional road traffic authorities that are involved in the project or can verify data. If trust in government is high, it would make end users confident that the data in the cardossier is genuine and that it can be trusted. The second possibility would be a label from a university. Research activities that underlie the development and bring transparency over it may enhance the trustworthiness of the whole platform. The third possibility sets a quality seal or a test report from an independent third party that specifically examines and audits blockchain platforms. To the authors' knowledge, no such body exists in Switzerland at the time of this work, however, there are several companies that have begun auditing blockchain platforms. With the increasing popularity and spread of such platforms, this is classified as a possibility for the future.

TSDE8 and TSDE9. Videos (instructional / comic)



Literature suggests that visual information in general, and short videos specifically, are more beneficial in trust building on websites [70]. The last two TSDEs show two different types of video, which are intended to increase trustworthiness in the cardossier by allowing the end user to visualize information about it. The first illustration represents a more traditional instructional video with an instructor explaining certain facts (e.g., how blockchain technology works or what the functionalities of the cardossier are). The second one is an example of an animated comic video that is intended to present facts as simply as possible, using graphics and drawings to represent a possible scenario (problem and solution) in which the cardossier may be useful.

A screenshot of the prototype, which was implemented as an instantiation of the designed TSDEs, can be found in Figure 5. This prototype was used for the second iteration of the evaluation. During the evaluation, the researcher could turn on and off the TSDEs to be tested.

This is the authors' version of the article. The printed journal version can be accessed at: https://ieeexplore.ieee.org/document/9199099/

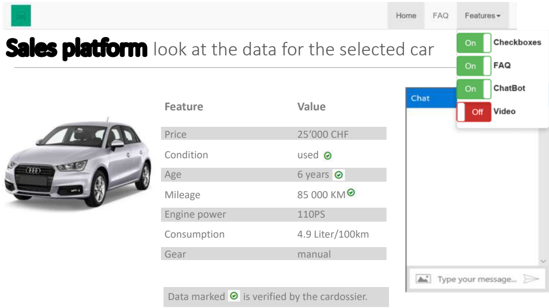


Figure 5. Evaluated cardossier app prototype

7. Evaluation

First iteration – Survey and Workshop

In this section we present the results of the evaluation of the designed TSDEs from the final evaluation. The ranking of the TSDEs from the survey is shown in the Table 1.

TSDE Name	Category	Rank
TSDE1. FAQ	Information	1
TSDE5. Governmental label	Labels	2
TSDE9. Comic video	Information	3
TSDE4. Chatbot	Information	4
TSDE6. University label	Labels	5
TSDE2. Tooltips	Information	6
TSDE3. Checkboxes	User interface	7
TSDE7. Certification label	Labels	8
TSDE8. Instructional video	Information	9

Table 1. Ranked TSDEs and their categories

The most relevant TSDE in terms of providing more understandability and trustworthiness was FAQ (TSDE1). Among the labels, the governmental label (TSDE5) (that the Road Traffic Authority approves or supports the platform) was considered much more important than a certification label (TSDE7) (e.g., that the platform was audited) and moderately more important than the label from a university (TSDE6). Comparing the comic video (TSDE9) and the instructional video (TSDE8), the comic video was widely welcomed by the participants. At that point, we didn't ask the participants to explain why, but this iteration helped us to identify the most welcomed TSDEs, that were later discussed in a workshop with the project team. In the workshop, checkboxes in particular were considered several times as useful, "*are* *a good eye-catcher*" (P6)[6] and thus arouse interest. In addition, tooltips have been considered several times as useful, not only to show information on the cardossier itself, but to explain more specific information in selected contents. If some data is shown in an aggregated form (e.g., the current mileage state and not each mileage record event), tooltips can be useful to explain how the data was aggregated where checkboxes are not appropriate. However, tooltips were considered overwhelming for end users when integrated in an online used-car sales platform. As a result, the final implementation did not include labels. Labels for the car-dossier were also intensively discussed. On the one hand, they were classified as interesting for end users and can attract the attention of the user if they recognize a certain reliable organization. Labels can also make valuable contributions to the security of the platform ("*for the security part we need a check or a label*" (P4)) and for data protection. On the other hand, important hurdles and limitations in the implementation of labels were mentioned, which led to them being excluded them from the final implementation. "*University of Zurich as a label will certainly not work. For legal reasons*" (P1). Realization of labels from other project partners is not that straight-forward. The challenge with this would be that the organization issuing the labels would have to somehow guarantee/check the data and the platform and assume liability. While labels are powerful for creation of trust, challenges related to institutional problems should be concerned and resolved first before labels can be implemented. However, it would be possible to "*use the cardossier itself as a label (...) and showing what percentage of data is cardossier verified*" (P1). The feedback regarding FAQ was relatively uncontroversial and the basic statements about them were as positive as those in the results of the surveys, "*FAQs are pretty well accepted*" (P6) or "*for me, FAQs are still the variant where I get the best answers*" (P10). The situation was different with the chatbot, which on the one hand was identified as high potential and worth trying out, but on the other hand opinions like "*I*

[6] The quotes here and further in the text are taken from the workshop (P) and interviews (T).

do not know what I can actually do with chatbots" (P10) were expressed. With the videos, the general consensus was clear that it's worth trying, but only in the form of animation/comic videos. A statement, made by one of the participants about traditional instructional videos, made it clear that they should no longer be used for such purposes. Finally, all TSDEs except for tooltips (TSDE2), labels (TSDE5-7) and instructional video (TSDE8) were implemented for the second iteration of the evaluation.

Second iteration – Evaluation with Users

This section describes the results of the final, second iteration of the evaluation. Table 2 shows how the designed TSDEs correspond to the addressed antecedents of trust, i.e. understandability, reliability, information accuracy.

Generic requirements		**Antecedents of trust [25]**	**TSDEs**					
			FAQ	Tooltips	Checkboxes	Chatbot	Labels	Videos
	Enable:	Understandability of the IT artifact	✓	✓		✓		✓
		Reliability of the IT artifact					✓	
		Information accuracy in the IT artifact			✓			

Table 2. TSDEs matched to proposed generic requirements

The interviews revealed certain tendencies regarding the popularity and readiness for use of the individual TSDEs. In seven out of nine interviews, the **FAQ (TSDE1)** was mentioned in response to the question "*Which component would you most likely use to search for more information?*". The FAQ was favored by the majority of participants, largely due to the fact that it is a widely recognized feature on websites. Participants welcomed the information in the FAQ: "*thinking that various questions have been covered in the FAQ (...) increases my confidence*" (T9). As a potential for improvement here, participants suggested communicating transparently what the interests of the individual stakeholders (an insurance company, a car-sharing company, etc.) in the project are. The **comic video (TSDE9)** also generally performed well. However, some participants wished to have more content in the video. The video provided basic information in a short time, which "*could give a good overview*" (T4) and makes it easier to arouse the interest of end users: "*Video stands out from the others*" (T3). However, few participants explicitly asked for more content to be made available in the video. However, it was recognized that it is important to ensure the video is not too long: the right length was considered to be around 90 seconds. The reaction to the **chatbot (TSDE4)** was mixed, from a single vote as first choice to some very negative attitudes. None of the participants regularly used chatbots. Six of the nine interviewees had never used a chatbot before. The mentioned experiences are neutral or negative: "*you ask in five different ways and you get the same answer every time*" (T7). However, there were positive comments about how "*to ask exactly what you need and actually get a short answer*" (T2) and some participants even preferred it to a conventional FAQ. This was especially noticeable among participants with little or no technical affinity, who were unfamiliar with chatbots. The **checkboxes (TSDE3)** were rated exclusively neutral or positive, with the neutral votes stating that the checkboxes in themselves offer little added value. Checkboxes alone cannot bring much value for trust and require an additional explanation of their purpose. The positive opinions, however, often implicitly required an initial trust in the cardossier.

8. Discussion and Conclusions

Our study demonstrates a possible set of TSDEs for blockchain platforms. Having conducted this study, we can make several observations. Firstly, we would like to confirm the problems identified by the literature (lack of understanding, knowledge and experience with the blockchain technology, which lead to lower levels of trust) that may be observed not only in studies of public blockchains (e.g., bitcoin, described in [6]), but also for those blockchain platforms where parties are known (permissioned blockchains developed by consortia), like in the case of the cardossier. Still, to a user who has less affinity with technology and is less trend-conscious, the trustworthiness of a platform should be communicated in a straightforward way to instill trust. In particular, support to develop understandability is a crucial antecedent of trust in the case of blockchain platforms [25]. To do that, existing mechanisms (like FAQ and videos) that users are already familiar with are very helpful [34]. In order to develop the understandability of a platform, information about its purpose and functionality should be provided. In the case of blockchain platforms, where data quality is an issue [31], information about data providers and their incentives to be a part of the system and to provide data can be especially relevant. Additionally, we noticed that a user-centered approach is helpful in designing such TSDEs. For example, in the FAQ, most of the questions are those that users would generate themselves. However, users may be not familiar with capabilities and specific characteristics that a technology has, like a decentralized and distributed operation of blockchain technology if it is not communicated proactively, and thus may have no concerns (like regarding data privacy in our case) that would probably occur if they had known this before. Therefore, we conclude that a user-centered approach should be combined with proactive communication about possible vulnerabilities of a system and how they are being addressed. Regulations (such as GDPR) can help and 'force' businesses to do this, and thus provide users with their 'right to explanation' [44].

The comic video was much more popular as it introduced a simple problem which any user would be familiar with (the purchase of a used car) and the solution the cardossier brings. This way, the user could relate to the situation much better and thus understand the purpose of the cardossier. In contrast, the chatbot produced an opposite effect. Most of the users were not familiar with its purpose and functionality, leading to negative experiences. Therefore, we conclude that not only the amount of information and level of detail provided is important for understandability [42, 45], but the way *how* it is provided. In our case, known instruments of trust support (e.g. an FAQ) were better suitable to generating trust than an unknown one (a chatbot): i.e. I trust the content of a TSDE because I already know its structure. In the case of blockchain platforms, the content of the TSDEs (such as the actual FAQs, videos, tooltips, etc.) should describe the unique value proposition of the blockchain technology itself (without going into technical details) and blockchain-based applications built on top of the platform. For example, one answer in the FAQ might describe the cardossier report as being hashed to prevent tampering and immutably recorded by multiple parties. Therefore, we conclude that known instruments could serve as a kind of trust anchor. This supports the discourse on relationship between familiarity and trust in IT, but from a new angle. Previous studies [36, 37] examine familiarity with an institution as a trust enhancing component. We suggest, that familiarity with individual design elements on the surface structure (i.e. the interface users interact with) help to improve overall trust in the system, or more specifically in our case, in a blockchain platform (the deep structure, defined by the purpose of the system, trusted vehicle's history in our case) [38–40]. With this, we argue that in order to enable the trustworthiness of blockchain-based applications on the deep structure level, the surface structure should be targeted and enhanced with TSDEs. Reflecting back about the cardossier's system architecture, we conclude that trust is created and transferred on different levels: the trust is "passed on" upwards over several levels and in addition, each level generates its own trust. In other words, to trust the cardossier system: a) one trusts the blockchain core as a technology, and b) one trusts the consortium, which develops only trustworthy applications (this fact is backed by brands and reputation of companies involved in the consortium), and c) one trusts partners to implement their use cases in a trustworthy manner. Altogether, these three trust levels are communicated to the end user through the surface structure (i.e. the cardossier's interface). This trust building, however, should be further studied to explore what happens in the case when trust on one of the levels is broken or cannot be properly communicated. Furthermore, future studies should focus on how the physical structure (for example, sensors for data input) should be designed to make the overall information system more trustworthy.

This brings us back to the question of whether or not blockchain platforms should be 'white-boxed' or 'black-boxed'. Our study confirms the fact that an explanation, provided to the user, should be meaningful and should have the 'right' level of detail, that is still comprehensive to the user [42]. However, in contrast to AI systems, discussed by [42, 45], blockchain systems do not intend to make any decision for the user, instead, they provide access to data that can be trusted due to certain characteristics of the technology (such as immutability, authentication). Therefore, we argue, that the explanation should be more data-centered, and focus on, first, providing enough information about data quality, and second, about privacy (which is a challenge of blockchain platforms [8, 10, 11]) and security.

Secondly, we argue that to make blockchain platforms more trustworthy, reliability (another antecedent of trust) should be addressed [30]. To do that, we designed several labels which verified that the data in the cardossier was genuine and showed users that the project was supported by one of several institutions. Though end users welcomed such labels, like the governmental or university labels, there are legal limitations in their implementation. Furthermore, they might be more or less useful for trust support depending on the level of trust in these institutions. Therefore, trust in a blockchain platform may increase or decrease by transfer of trust from institutions to platform. In countries where there is no trust in government, usage of a governmental label will not increase the level of trust and might, in fact, be a negative influence. Furthermore, labels can be ambivalent as TSDEs. A government is trustworthy because it does not normally facilitate the transfer of trust into commercial companies. Therefore, there are certain prerequisites for the 'governmental' institutional trust, that can be instilled by the government, involved in the development efforts. In the case of the Cardossier project, a non-profit association was founded, among other factors, to address this prerequisite. Yet it remains open in which form the Swiss government can give its name to support the Cardossier. On the other hand, a new label to be trustworthy have to be established on the market first. The companies, involved in the arrangement in the Cardossier project, could manage this with some joint effort. But, given the joint creation and the distributed governance of the cardossier platform [50, 51], the question is whether they are ready to share their reputation and trustworthiness with each other to create a more trustworthy platform to jointly benefit from it [50]. Thus, we can conclude that institutional trust [1], especially trust created by a governmental authority, can help establish trustworthiness of a blockchain platform [71]. This conclusion brings us back to the question whether blockchain platforms mediate and support trust relationships between humans and institutions [25] or other way around: to be able to build a blockchain platform and utilize its potential, the blockchain platform should be backed by inter-personal and institutional trust relationships. This triad between inter-personal, institutional, and trust in IT in relation to blockchain platforms should be studied further. Furthermore, as mentioned before, trust in blockchain platforms differs in the sense that the role of platform provider changes. Instead of having one trusted party, there might be many (like a blockchain consortium in the case of the cardossier) with different levels of trust. This shift should be certainly studied further. Additionally, we see a potential for blockchain platforms, which are perfectly suited for authentication purposes [7], to issue trust labels by themselves and, by doing so, create a new business model.

Thirdly, we aimed to provide information accuracy (the last antecedent of trust we addressed). Though we have seen a positive reaction to the designed TSDE checkboxes, their use is limited to platforms that integrate data from a blockchain platform, like the used-car sales platform in our case, with the integrated data from the cardossier. Though visually appealing, checkboxes in the cardossier itself would not make much sense. Furthermore, an initial level of trust in the cardossier is still needed to ensure confidence in these checkboxes, as reported by participants of our study. Thus, we encourage researchers to continue design studies on trust for blockchain platforms.

Altogether, the identified TSDEs can be seen as trust signals, demonstrating (signaling) trustworthiness of the IT artifact to an end user. As the literature suggests [28], good signals are easy to create in terms of their cost structure. In our case, such signals as FAQ or a comic video can be viewed as good signals as their creation requires transparent documentation of its operation (as opposed to an untrustworthy provider which would invest much effort into composing a legitimate story). Similarly, visualizing brands of organizations, standing behind the cardossier, on an interface would be easy as they are part of the project and agree to contribute (as opposed to an untrustworthy provider using brands of organizations with a good reputation that never agreed to this usage, which will quickly lead to a court case).

All in all, our study makes the following contribution to design science and information systems discourse on trust creation for blockchain platforms: we demonstrate, how TSDEs can be designed to foster end-user trust in a blockchain platform and discuss implications of such a design. We admit that the contribution of our study focuses solely on TSDEs applicable to permissioned blockchain platforms, where parties are known. Furthermore, these TSDEs are designed for the surface structure of an information system (i.e. the interface) which is able to properly communicate the trustworthiness of the deep structure of the information system. Thus, with this study, we show how well-known and recognized design elements may bring value and communicate trustworthiness in the design of novel systems that promise to bring trust by design.

This research has following limitations: we acknowledge that the number of participants in both surveys and the interview for the final evaluation does not allow for generalizable conclusions about which TSDEs are the most effective in building trust, however, we believe in the strength of the discussed needs and requirements for explanation from the end users' perspective. Furthermore, in our case, the integration of the cardossier in a used-car sales platform was necessary to make the situation more familiar to the users. However, it is important to study what effect TSDEs have when the use of the cardossier is isolated from the used-car sales platform. Additionally, it is worthwhile to search and develop further TSDEs for blockchain platforms that are not covered in this study. These may be TSDEs which proved to be powerful in other contexts or completely new ones. We acknowledge that our research was designed the way that we could not create completely new TSDEs, but we rather sought for finding out what existing ones are appropriate for blockchain platforms. Concerning future research, we see potential in developing studies that examine user perception of blockchain platforms, their trustworthiness, and the acceptance of these platforms.

9. References

1. Son, J.-Y., Tu, L., Benbasat, I.: A descriptive content analysis of trust-building measures in B2B electronic marketplaces. Communications of the Association for Information Systems. 18, 6 (2006).
2. Fleischmann, M., Ivens, B.: Exploring the Role of Trust in Blockchain Adoption: An Inductive Approach. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (2019).
3. Seebacher, S., Schüritz, R.: Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review. In: Za, S., Drăgoicea, M., and Cavallari, M. (eds.) Exploring Services Science. pp. 12–23. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-56925-3_2.
4. Beck, R., Stenum Czepluch, J., Lollike, N., Malone, S.: Blockchain–The Gateway To Trust-Free Cryptographic Transactions. Twenty-Fourth European Conference on Information Systems (ECIS). (2016).
5. Notheisen, B., Cholewa, J.B., Shanmugam, A.P.: Trading Real-World Assets on Blockchain. Bus Inf Syst Eng. 59, 425–440 (2017). https://doi.org/10.1007/s12599-017-0499-8.
6. Sadhya, V., Sadhya, H., Hirschheim, R., Watson, E.: Exploring technology trust in bitcoin: the blockchain exemplar. (2018).
7. Miscione, G., Ziolkowski, R., Zavolokina, L., Schwabe, G.: Tribal governance: The business of blockchain authentication. In: Prepared for the Hawaii International Conference on System Sciences (HICSS) (2018).
8. Elsden, C., Manohar, A., Briggs, J., Harding, M., Speed, C., Vines, J.: Making Sense of Blockchain Applications: A Typology for HCI. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery (ACM), New York (2018).
9. Ostern, N., Cabinakova, J.: Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems. Presented at the January 8 (2019).
10. Ostern, N.: Do You Trust a Trust-Free Transaction? Toward a Trust Framework Model for Blockchain Technology. Presented at the International Conference of Information Systems (ICIS) (2018).

11. Schlegel, M., Zavolokina, L., Schwabe, G.: Blockchain Technologies from the Consumers' Perspective: What Is There and Why Should Who Care? In: Proceedings of the 51st Hawaii International Conference on System Sciences (2018).
12. Koens, T., Poll, E.: The Drivers Behind Blockchain Adoption: The Rationality of Irrational Choices. In: European Conference on Parallel Processing. pp. 535–546. Springer (2018).
13. Söllner, M., Hoffmann, A., Hoffmann, H., Leimeister, J.M.: How to use behavioral research insights on trust for HCI system design. In: CHI'12 Extended Abstracts on Human Factors in Computing Systems. pp. 1703–1708. ACM (2012).
14. Morabito, V.: Business Innovation Through Blockchain. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-48478-5.
15. Leimeister, J.M., Ebner, W., Krcmar, H.: Design, Implementation, and Evaluation of Trust-Supporting Components in Virtual Communities for Patients. JMIS. 21,.
16. Lee, J.D., See, K.A.: Trust in Automation: Designing for Appropriate Reliance. (2004).
17. Faems, D., Janssens, M., Madhok, A., Looy, B.V.: Toward an integrative perspective on alliance governance: Connecting contract design, trust dynamics, and contract application. Academy of management journal. 51, 1053–1078 (2008).
18. Mayer, R.C., Davis, J.H., Schoorman, F.D.: An integrative model of organizational trust. Academy of management review. 20, 709–734 (1995).
19. Dirks, K.T., Ferrin, D.L.: The role of trust in organizational settings. Organization science. 12, 450–467 (2001).
20. Lewis, W., Agarwal, R., Sambamurthy, V.: Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. MIS quarterly. 657–678 (2003).
21. Williamson, O.E.: Markets and hierarchies. New York. 2630, (1975).
22. Williamson, O.E.: Calculativeness, trust, and economic organization. The journal of law and economics. 36, 453–486 (1993).
23. Zaheer, A., McEvily, B., Perrone, V.: Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance. Organization science. 9, 141–159 (1998).
24. Söllner, M., Hoffmann, A., Leimeister, J.M.: Why different trust relationships matter for information systems users. European Journal of Information Systems. 25, 274–287 (2016).
25. Söllner, M., Hoffmann, A., Hoffmann, H., Wacker, A., Leimeister, J.M.: Understanding the formation of trust in IT artifacts. Presented at the International Conference on Information Systems (2012).
26. Hoffmann, A., Hoffmann, H., Söllner, M.: Fostering initial trust in applications–developing and evaluating requirement patterns for application websites. In: 21st European Conference on Information Systems (ECIS), Utrecht, The Netherlands (2013).
27. Hoffmann, A., Söllner, M., Hoffmann, H., Leimeister, J.M.: Towards trust-based software requirement patterns. In: Requirements Patterns (RePa), 2012 IEEE Second International Workshop on. pp. 7–11. IEEE (2012).
28. Riegelsberger, J., Sasse, M.A., McCarthy, J.D.: The mechanics of trust: A framework for research and design. International Journal of Human-Computer Studies. 62, 381–422 (2005).
29. Loebbecke, C., Lueneborg, L., Niederle, D.: Blockchain Technology Impacting the Role of Trust in Transactions: Reflections in the Case of Trading Diamonds. In: European Conference on Information Systems (ECIS) (2018).
30. Lemieux, V.L.: Trusting records: is Blockchain technology the answer? Records Management Journal. 26, 110–139 (2016). https://doi.org/10.1108/RMJ-12-2015-0042.
31. Zavolokina, L., Spychiger, F., Tessone, C., Schwabe, G.: Incentivizing Data Quality in Blockchains for Inter-Organizational Networks – Learning from the Digital Car Dossier. Presented at the International Conference of Information Systems (ICIS) (2018).
32. Zavolokina, L., Miscione, G., Schwabe, G.: Buyers of Lemons: Addressing Buyers' Needs in the Market for Lemons with Blockchain Technology. In: 52nd Hawaii International Conference on System Sciences. p. 10 (2018).
33. Sadhya, V., Sadhya, H.: Barriers to Adoption of Blockchain Technology. (2018).
34. Auinger, A., Riedl, R.: Blockchain and Trust: Refuting Some Widely-held Misconceptions. Presented at the International Conference of Information Systems (ICIS) (2018).
35. Li, X., Rong, G., Thatcher, J.B.: Do we trust the technology? People? or both? Ruminations on technology trust. AMCIS 2009 Proceedings. 459 (2009).
36. Gulati, R., Sytch, M.: Does familiarity breed trust? Revisiting the antecedents of trust. Managerial and Decision Economics. 29, 165–190 (2008).
37. Komiak, S.Y., Benbasat, I.: The effects of personalization and familiarity on trust and adoption of recommendation agents. MIS quarterly. 941–960 (2006).

38. Burton-Jones, A., Grange, C.: From use to effective use: a representation theory perspective. Information systems research. 24, 632–658 (2012).
39. Weber, R.: Ontological foundations of information systems. Coopers & Lybrand and the Accounting Association of Australia and New … (1997).
40. Wand, Y., Weber, R.: Toward a theory of the deep structure of information systems. In: ICIS. p. 3 (1990).
41. Öksüz, A., Walter, N., Pfeiffer, T., Becker, J.: Designing Trust in Websites-an Evaluation of Leading Infrastructure as a Service Providers' Websites. In: PACIS. p. 357 (2014).
42. Pieters, W.: Explanation and trust: what to tell the user in security and AI? Ethics and information technology. 13, 53–64 (2011).
43. Bouchagiar, G.: Initial Coin Offering and Cryptocurrencies: Shifting Trust Away from Human Actors and toward a Cryptographic System. Journal of Financial Risk Management. 7, 386–427 (2018).
44. Kim, T.W., Routledge, B.: Algorithmic transparency, a right to explanation and trust. (2017).
45. Kizilcec, R.F.: How much information?: Effects of transparency on trust in an algorithmic interface. In: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. pp. 2390–2395. ACM (2016).
46. Akerlof, G.A.: The market for "lemons": Quality uncertainty and the market mechanism. The quarterly journal of economics. 488–500 (1970).
47. Notheisen, B., Cholewa, J.B., Shanmugam, A.P.: Trading Real-World Assets on Blockchain: An Application of Trust-Free Transaction Systems in the Market for Lemons. Business & Information Systems Engineering. 59, 425–440 (2017).
48. Bauer, I., Zavolokina, L., Schwabe, G.: Is there a market for trusted car data? Electronic Markets. 1–15 (2019).
49. Sein, M.K., Henfridsson, O., Purao, S., Rossi, M., Lindgren, R.: Action design research. MIS quarterly. 37–56 (2011).
50. Bauer, I., Zavolokina, L., Leisibach, F., Schwabe, G.: Exploring Blockchain Value Creation: The Case of the Car Ecosystem. In: Proceedings of the 52th HICSS. (2018).
51. Ziolkowski, R., Miscione, G., Schwabe, G.: Consensus through Blockchains: Exploring Governance across inter-organizational Settings. In: ICIS 2018 Proceedings. , San Francisco, CA, USA (2018).
52. Ziolkowski, R., Parangi, G., Miscione, G., Schwabe, G.: Examining Gentle Rivalry: Decision-Making in Blockchain Systems. In: HICSS 2019 Proceedings. , Maui, Hawaii, USA (2019). http://hdl.handle.net/10125/59891.
53. Zavolokina, L., Ziolkowski, R., Bauer, I., Schwabe, G.: Management, Governance and Value Creation in a Blockchain Consortium. Forthcoming in MISQE. (2020).
54. Zavolokina, L., Schlegel, M., Schwabe, G.: How Can We Reduce Information Asymmetries and Enhance Trust in 'The Market for Lemons'? Conditionally accepted at Information Systems and e-Business Management Journal (ISeBM). (2019).
55. Hevner, A.R., March, S.T., Park, J., Ram, S.: Design Science in Information Systems Research. MIS Quarterly. No. 1, 75–105 (2004).
56. Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S.: A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24, 45–77 (2007). https://doi.org/10.2753/MIS0742-1222240302.
57. Baskerville, R., Pries-Heje, J., Venable, J.: Soft design science methodology. In: Proceedings of the 4th international conference on design science research in information systems and technology. p. 9. ACM (2009).
58. Nunamaker, J.F., Briggs, R.O., Derrick, D.C., Schwabe, G.: The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research. Journal of Management Information Systems. 32, 10–47 (2015).
59. Anderson, J., Donnellan, B., Hevner, A.: Exploring the relationship between design science research and innovation: a case study of innovation at Chevron. In: European Design Science Symposium. pp. 116–131. Springer (2011).
60. Maedche, A., Gregor, S., Morana, S., Feine, J.: Conceptualization of the Problem Space in Design Science Research. In: International Conference on Design Science Research in Information Systems and Technology. pp. 18–31. Springer (2019).
61. Bider, I., Johannesson, P., Perjons, E., Johansson, L.: Design science in action: developing a framework for introducing IT systems into operational practice. (2012).
62. Lee, J.S., Pries-Heje, J., Baskerville, R.: Theorizing in design science research. In: International Conference on Design Science Research in Information Systems. pp. 1–16. Springer (2011).
63. Brown, T., Wyatt, J.: Design thinking for social innovation. Development Outreach. 12, 29–43 (2010).
64. Hevner, A.R.: A three cycle view of design science research. Scandinavian journal of information systems. 19, 4 (2007).

65. Saldaña, J.: The coding manual for qualitative researchers. Sage, Los Angeles, Calif (2009).
66. Collier, J.E., Bienstock, C.C.: How do customers judge quality in an e-tailer? MIT Sloan Management Review. 48, 35 (2006).
67. Vinkovits, M., Zimmermann, A.: Defining a trust framework design process. In: International Conference on Trust, Privacy and Security in Digital Business. pp. 37–47. Springer (2013).
68. Jenkins, M.-C., Churchill, R., Cox, S., Smith, D.: Analysis of user interaction with service oriented chatbot systems. In: International Conference on Human-Computer Interaction. pp. 76–83. Springer (2007).
69. Grabner-Kraeuter, S.: The role of consumers' trust in online-shopping. Journal of Business Ethics. 39, 43–50 (2002).
70. Chen, L., Pu, P.: Trust building in recommender agents. In: Proceedings of the Workshop on Web Personalization, Recommender Systems and Intelligent User Interfaces at the 2nd International Conference on E-Business and Telecommunication Networks. pp. 135–145. Citeseer (2005).
71. Son, J.-Y., Tu, L., Benbasat, I.: A descriptive content analysis of trust-building measures in B2B electronic marketplaces. Communications of the Association for Information Systems. 18, 6 (2006).

10. Appendix

Code	Segment
Trust factors\Data-related\Data manipulability\Falsification	B: So if they can't be falsified, then it's definitely trustworthy, I'd say. But you can also falsify them if you have a friend who has a garage. He can then manipulate the data a little. That is the weak point of the whole thing.
	B: Yes, it's secure and unfalsifiable, and it's also meant to be like a blockchain. Apply correctly. So the application simply has to be correct.
	B: Well, I don't really know much about blockchain but I think it's pretty difficult to manipulate things there without really being authorized to do so, so I would probably trust the blockchain more.
	B: Because if you are honest, people look at some signature and if the signature is real or not, you can't tell in case of doubt, that's why I would have fewer concerns, if, let me say, IT was well covered from a security point of view.

Table 3. Example coded segments for the sub-code Falsification